PROCEDE DE CHIFFREMENT DE DONNEES, SYSTEME CRYPTOGRAPHIQUE ET COMPOSANT ASSOCIES

L'invention concerne un procédé de chiffrement, et un système cryptographique associé, avec application notamment dans le domaine de la cryptographie à clé publique. L'invention peut être mise en œuvre dans des dispositifs électroniques tels que des cartes à puce.

Un système cryptographique à clé publique complet comprend généralement un algorithme de chiffrement et un algorithme de signature. Un tel système cryptographique peut être mis en œuvre par exemple dans une carte à puce comprenant notamment, dans un circuit intégré, des moyens de calcul programmés pour mettre en œuvre les algorithmes, et des moyens de mémorisation, pour mémoriser des clés publiques et / ou des clés secrètes nécessaires à la mise en œuvre des algorithmes.

Un algorithme connu et utilisé dans les systèmes cryptographiques à clé publique est l'algorithme RSA (de Rivest, Shamir et Adleman). Il peut être utilisé pour réaliser des opérations de chiffrement et des opérations de signature. De manière général, l'algorithme RSA consiste à réaliser une opération d'exponentiation, à l'aide d'une clé publique ou privée, d'un message clair formaté par une fonction de chiffrement ou une fonction de signature, selon le cas.

Un procédé de chiffrement utilisant l'algorithme RSA consiste ainsi à formater un message clair m par une fonction de chiffrement μ, puis à réaliser une exponentiation du résultat selon la relation :

$$c = f(\mu(m)) = [\mu(m)]^e \bmod N$$

où μ est une fonction de chiffrement, (N, e) une clé publique, et f(x, N, e) la fonction d'exponentiation $f(x, N, e) = x^e \bmod N$.

Le message chiffré c peut ensuite être déchiffré en

utilisant à nouveau l'algorithme RSA, avec la fonction inverse $f^{-1}(x, N, d)$, (N, d) étant une clé privée associée à la clé publique (N, e).

Un procédé de signature utilisant l'algorithme RSA consiste manière similaire à formater un message clair m par une fonction de signature μ', puis à réaliser une exponentiation du résultat selon la relation :

$$s = f^{-1}[\mu'(m)] = [\mu'(m)]^{d'} \bmod N'$$

où μ' est une fonction de signature, (N', d') une clé privée, et $f^{-1}(x, N', d')$ la fonction d'exponentiation $f^{-1}(x, N', d') = x^{d'} \bmod N'$.

La signature peut ensuite être vérifiée en utilisant à nouveau l'algorithme RSA, avec la fonction inverse f(x, N', e'), (N', e') étant une clé publique associée à la clé privée (N', d').

Les fonctions d'exponentiation et les fonctions de chiffrement ou de signature utilisées dans les systèmes cryptographiques sont en général connues. La sécurité des systèmes de cryptage dépend donc uniquement des clés privées et publiques utilisées, qu'il est indispensable de maintenir cachées.

La sécurité dépend ainsi notamment de la taille des clés, qui sont choisies de grande taille. Les nombres N, N' sont généralement de grande taille, par exemple 1024 bits, ils sont égaux au produit de deux nombres premiers N = p*q, N' = p'*q'. Les nombres d, d' entiers dépendent des nombres N, N' et sont également de grande taille. Les nombres e, e' entiers sont par contre souvent de petite taille.

Pour des raisons de sécurité, les clés ((N, e) ; (N, d)) utilisées pour le chiffrement et les clés ((N', e') ; (N', d')) utilisées pour la signature sont différentes.

Une fonction de signature μ' est dite sûre s'il n'est pas possible de créer une signature s d'un message m sans connaître la clé privée, même si des signatures

s1, s2 de messages m1, m2 sont connues. Les fonctions μ' utilisées dans les systèmes cryptographiques sont construites pour vérifier cette condition.

Une fonction μ' connue et sûre pour des opérations de signature est la fonction PSS (Probabilistic Signature Scheme, en français fonction probabiliste de signature), décrite notamment dans le document D1 (M. Bellare and P. Rogaway, The exact security of digital signatures- How to sign with RSA and Rabin, Proceedings of Eurocrypt'96, LNCS vil 1070, Springer-Verlag, 1996, pp 399-416) et dans le standard PKCS#1 v2.1, RSA Cryptography Standard.

La fonction PSS est paramétrée par des entiers k, k0, k1 et utilise deux fonctions de hachage :

$$H : \{0, 1\}^{k-k1} \rightarrow \{0, 1\}^{k1}$$

$$G : \{0, 1\}^{k1} \rightarrow \{0, 1\}^{k-k1}$$

A partir d'un texte clair m de k - k0 - k1 bits et d'un nombre r aléatoire de k0 bits, la fonction PSS produit :

$$PSS(m, r) = \omega \,||\, s$$

avec r un paramètre aléatoire associé à la fonction PSS, $||$ la fonction de concaténation, $\omega = H(m \,||\, r)$, $s = G(\omega) \oplus (m \,||\, r)$, et $\oplus$ la fonction logique XOR.

La signature s du message m est ensuite obtenue par exponentiation à l'aide de la clé secrète (N, d) :

$$s = f([PSS(m, r)], N, d)$$
$$= [PSS(m, r)]^d \bmod N$$

Une signature s peut être vérifiée en calculant :

$$f^{-1}(s) = s^e \bmod N = \omega \,||\, s$$

où f^{-1} est la fonction inverse de la fonction d'exponentiation f.

Connaissant la taille de ω et s (respectivement k1 bits et k-k1 bits), on déduit ω et s de $f^{-1}(s)$. On calcule ensuite $G(\omega) \oplus s$ à partir de ω, s et G. Comme $G(\omega) \oplus s = M \,||\, r$, on en déduit finalement $H(m \,||\, r)$ et m. Enfin, on compare ω et $H(m \,||\, r)$. Si $H(m \,||\, r) = \omega$, alors le texte clair m est renvoyé, sinon seul un message

d'erreur est renvoyé.

De manière similaire, une fonction μ de chiffrement est dite sûre s'il n'est pas possible de distinguer deux messages chiffrés c1, c2 obtenus à partir de la fonction μ et de deux messages clairs m1, m2, même si l'un des messages clairs associés m1 ou m2 est connu. Les fonctions μ utilisées dans les systèmes cryptographiques sont construites pour vérifier cette condition de sécurité.

Cependant, parce que les critères de sécurité ne sont pas les mêmes pour des opérations de signature et des opérations de chiffrement, les fonctions μ' de signature et les fonctions μ de chiffrement ne sont pas les mêmes.

En conséquence, pour implémenter un système cryptographique complet, apte à chiffrer et déchiffrer, il est nécessaire de disposer de moyens pour mémoriser deux fonctions différentes, plus généralement deux algorithmes différents, et de disposer de moyens de calcul programmés différents pour les mettre en œuvre. La taille du circuit électronique résultant est bien évidemment proportionnelle à la taille des algorithmes à mémoriser.

Pour résoudre le problème évoqué ci-dessus, selon l'invention, on utilise une même fonction de formatage, à la fois comme fonction de chiffrement et comme fonction de signature. Plus précisément, selon l'invention, pour mettre en œuvre un procédé de chiffrement, on utilise la fonction PSS, connue par ailleurs pour mettre œuvre un procédé de signature.

Ainsi, l'invention concerne un procédé de chiffrement, comprenant une étape de formatage d'un message clair par une fonction de formatage, et une étape

d'exponentiation du résultat de l'étape précédente à l'aide d'une clé publique selon la relation $c = \mu(m)^e \bmod N$, c étant un message chiffré, $\mu(m)$ étant le résultat de l'étape de formatage, et e et N des éléments de la clé publique.

Selon l'invention, la fonction de formatage est la fonction PSS.

La fonction PSS est une fonction sûre pour des opérations de chiffrement. En effet, il on montre que la fonction PSS est sûre pour des opérations de chiffrement, dans le modèle oracle aléatoire, tel que défini dans D2 : M. Bellare and P. Rogaway, Random oracles are practical : a paradigm for designing efficient protocols. Proceedings of the First Annual Conference on Computer Communication Security, ACM, 1993. Par ailleurs, actuellement dans le domaine de la cryptographie, la notion de sécurité dans le modèle oracle aléatoire et la notion de sécurité la plus forte pour des applications réelles.

Ainsi, selon l'invention, on dispose d'une fonction sûre à la fois pour des opérations de signature et de chiffrement.

L'invention concerne également un système de cryptographie comprenant un procédé de chiffrement et un procédé de signature, tous deux utilisant la fonction PSS comme fonction de formatage.

Plus précisément, le système cryptographique comprend :

- une étape de formatage d'un message clair par la fonction probabilistique de signature (PSS), puis :
- si un chiffrement du message clair est souhaité, une étape d'exponentiation du résultat de l'étape de formatage à l'aide d'une première clé selon la relation $c = \mu(m)^e \bmod N$, c étant un message chiffré, $\mu(m)$ étant le résultat de l'étape de formatage, et e et N des éléments de la première clé, ou
- si une signature du message clair est souhaitée,

une étape d'exponentiation du résultat de l'étape de formatage à l'aide d'une deuxième clé (N', d') selon la relation $s = \mu(m)^{d'} \bmod N'$, s étant un message signé, $\mu(m)$ étant le résultat de l'étape de formatage, et d' et N' des éléments de la deuxième clé.

Un tel système cryptographique est avantageux par rapport aux systèmes cryptographiques connus, dans la mesure où il nécessite environ deux fois moins de moyens (en termes de moyens de calcul programmés et de place mémoire notamment) pour être mis en œuvre.

Selon un mode de réalisation, la première clé et la deuxième clé sont respectivement une clé publique d'une première paire de clés et une clé privée d'une deuxième paire de clés.

Selon un autre mode de réalisation, préféré, la première paire de clé et la deuxième paire de clés sont identiques. En d'autres termes, le même jeu de clés est utilisé, à la fois pour mettre en œuvre le procédé de chiffrement et le procédé de signature. On montre en effet que déchiffrer un message, chiffré selon un procédé de chiffrement utilisant la fonction PSS et un jeu de clés donné, ne permet pas d'obtenir une information suffisante pour signer un message (éventuellement le message déchiffré) selon un procédé de signature utilisant la fonction PSS et le même jeu de clés. De manière symétrique, on montre qu'obtenir une information sur la signature d'un message signé, selon un procédé de signature utilisant la fonction PSS et un jeu de clés donné, ne permet pas d'obtenir une information sur un message clair chiffré selon un procédé de chiffrement utilisant la même fonction PSS et le même jeu de clés.

L'invention est notamment applicable à l'algorithme de cryptographie RSA, qui est l'algorithme le plus utilisé à ce jour dans le domaine de la cryptographie.

L'invention concerne également un composant électronique comprenant des moyens programmés pour la

mise en œuvre d'un procédé de chiffrement tel que décrit ci-dessus, utilisant la fonction PSS comme fonction de formatage. Les moyens programmés comprennent notamment une unité centrale et une mémoire de programme.

L'invention concerne encore un composant électronique comprenant des moyens programmés pour la mise en œuvre d'un système cryptographique tel que décrit ci-dessus, comprenant une opération de chiffrement ou une opération de signature, exécutées alternativement. Les moyens programmés comprennent notamment une unité centrale et une mémoire de programme.

L'invention est notamment intéressante pour des applications de type carte à puce, dans lesquels les composants utilisés doivent être de taille la plus petite possible, et la mise en œuvre des procédés la plus rapide possible.

REVENDICATIONS

1. Procédé de chiffrement, comprenant une étape de formatage d'un message clair (m) par une fonction de formatage (μ), et une étape d'exponentiation du résultat de l'étape précédente à l'aide d'une clé publique (N, e) selon la relation $c = \mu(m)^e \bmod N$, c étant un message chiffré, $\mu(m)$ étant le résultat de l'étape de formatage, et e et N des éléments de la clé publique,

le procédé étant caractérisé en ce que la fonction de formatage (μ) est la fonction PSS.

2. Procédé selon la revendication 1, caractérisé en ce que la fonction de formatage μ est définie par

$\mu(m) = PSS(m) = \omega \,||\, s$, avec :

m, le texte clair de k - k0 - k1 bits, r un paramètre aléatoire de k0 bits, k, k0, k1 étant des paramètres de la fonction de formatage,

||, une fonction de concaténation

$\omega = H(m \,||\, r)$

$s = G(\omega) \oplus (m \,||\, r)$,

$\oplus$ une fonction logique XOR, et

H, G deux fonctions de hachage

3. Utilisation d'une fonction probabilistique de signature (PSS) définie selon le standard PKCS#1 v2.1, RSA Cryptography Standard comme fonction de formatage (μ), pour réaliser un procédé de chiffrement comprenant une étape de formatage d'un message clair (m) par la fonction de formatage (μ), et une étape d'exponentiation du résultat de l'étape précédente à l'aide d'une clé publique (N, e) selon la relation $c = \mu(m)^e \bmod N$, c étant un message chiffré, $\mu(m)$ étant le résultat de l'étape de formatage, et e et N des éléments de la clé publique.

4. Système cryptographique, comprenant :

- une étape de formatage d'un message clair (m) par la fonction probabilistique de signature (PSS), puis :

- si un chiffrement du message clair (m) est souhaité, une étape d'exponentiation du résultat de l'étape de formatage à l'aide d'une première clé (N, e) selon la relation $c = \mu(m)^e \bmod N$, c étant un message chiffré, $\mu(m)$ étant le résultat de l'étape de formatage, et e et N des éléments de la première clé, ou

- si une signature du message clair (m) est souhaitée, une étape d'exponentiation du résultat de l'étape de formatage à l'aide d'une deuxième clé (N', d') selon la relation $s = \mu(m)^{d'} \bmod N'$, s étant un message signé, $\mu(m)$ étant le résultat de l'étape de formatage, et d' et N' des éléments de la deuxième clé.

5. Système selon la revendication 3, dans lequel la première clé et la deuxième clé sont respectivement une clé publique d'une première paire de clés et une clé privée d'une deuxième paire de clés.

6. Système selon la revendication 4, dans lequel la première paire de clé et la deuxième paire de clés sont identiques.

7. Système selon l'une des revendications 4 à 6, de type RSA.

8. Composant électronique comprenant des moyens programmés pour la mise en œuvre d'un procédé de chiffrement selon l'une des revendications 1 à 2, les moyens programmés comprenant notamment une unité centrale et une mémoire de programme.

9. Composant électronique comprenant des moyens programmés pour la mise en œuvre d'un système

cryptographique selon l'une des revendications 4 à 7, les moyens programmés comprenant notamment une unité centrale et une mémoire de programme.

10. Carte à puce comprenant un composant électronique selon la revendication 7 ou la revendication 8.